Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1611 03/14/14

~ Pay XP Users To Switch ~ People Are Talking! ~ Mt. Gox Death Spiral!
~ NSA Posed as Facebook! ~ Twitter Service Outage! ~ New Asus Chromebox!
~ How To Avoid Phishing! ~ Wordpress Sites Used! ~ WhatsMyBrowser.org!

~ Facebook HQ Evacuated! ~ Berners-Lee View on Web ~ PS4 Sales Tops Xbox!

-* Target Admits Missing Signs! *-
-* Digging for Atari's Corporate Shame *-
-* NSA "Hijacked" Criminal Botnets for Spyware *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

This winter weather just won't quit! Sure, we're supposed to hit 50 degrees this weekend, but it will be short-lived and return to frigid temperatures in a matter of a day or two. Personally, I've had enough!

Lots of great news and articles for you this week. In fact, we even have some retro-Atari tidbits for you - bringing back some great memories, I'm sure!

So, let's get right to this week's issue in order for you to read everything!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Mozilla, Epic Games Fast-tracking Web-based Gaming
""""""""""""""""""""""""""""""""
Next Angry Birds A Turn-based RPG!
Digging for Atari's 'Corporate Shame'!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Mozilla & Epic Games Are Fast-tracking Web-based Gaming

Web-based video games have been second-class citizens pretty much since their inception. And if one institution has a shot at changing that, it s Mozilla.

Mozilla is announcing today that it has partnered up once again with Epic Games, the makers of the most-used middleware in gaming. The two companies are bringing the Unreal Engine 4 framework to the web just in time for the Game Developers Conference next week in San Francisco.

Last year, Mozilla and Epic ported Unreal Engine 3 to the web, but the companies only demonstrated it at the conference as a proof-of-concept. This year, the technology is actually ready and available for developers to start building on.

Why is this important? A recent survey showed that 52 percent of Americans play browser-based games.

Much of the technology industry has been shifting to the web from desktop or native mobile software. Naturally, there s also been a high demand for more portable gaming technology, namely technology that makes games accessible through the browser. We say it s more portable because it works across all platforms, enabling you to take your gameplay from device to device, regardless of what that device is.

And these games are getting bigger in both size and scope. Our GamesBeat channel recently gave a web game, the role-playing/collectible card game Card Hunter, a high score.

During a call with VentureBeat, Mozilla engineering director and inventor of WebGL, Vlad Vukicevic, shared that the company has been working on making the Web ready for the next generation of games, especially ensuring that the experience in the browser rivals or at least matches that of native games.

Mozilla has been developing asm.js, a low-level subset of JavaScript with a special focus on speed and performance. As we previously reported, asm.js brought web-based performance a great deal closer to native software performance key attributes in making web gaming as close to the native experience as possible.

Vukicevic and Martin Best, Mozilla s game platform strategist, were happy to announce that the team has now gotten asm.js s speed down to 1.5 times that of native applications. It was twice as slow a year ago and five to 10 times slower when web-based gaming started to take off.

And although Mozilla s Firefox browser is currently most optimized for asmj.js, Chrome and Opera have been coming quite close to its levels recently.

Best also pointed out the implication this has for the gaming business. In the past, browser-based gaming required that users download plug-ins for high-end, 3D experiences, causing a high amount of friction and the loss of players who were not comfortable downloading them.

Removing this step greatly improves player draw and retention.

Increasing mobility making code that can run on any machine or operating system is also a huge advantage of putting games in the browser, Best added.

Monster Madness, the first commercial Unreal Engine 3 game published on the Web, saw immediate success when its maker, NomNom Games, released it.

Jeremy Stieglitz, NomNom Games chief technology officer, shared with

VentureBeat that since its release, half of the game s players have come from the Web.

Additionally, only about half of the web players have since switched to the native version, showing that the web release is both effective as a marketing tool but also a final destination for [more casual] users.

Since the first web release of Monster Madness was a direct copy of the native version of the game, NomNom Games is now releasing an even newer version, this time explicitly designed for the browser. The game will be live through the end of GDC and then will be periodically updated until a permanent version is released in May 2014.

As Mozilla heads into one of the biggest gaming conferences next week, it looks forward to showing off this year s proof-of-concept web gaming on mobile and plans to make it ship-worthy in the coming year.

Epic Games Unreal Engine powers some of the biggest franchises in the video games industry, including first-person shooter BioShock Infinite in the living room and action-role-playing game Infinity Blade on mobile.

Next Angry Birds A Turn-based RPG

If you wanted more bird-flinging, it looks like you might be in for a wait: the next title from Rovio to bear the Angry Birds brand is set to be a turn-based RPG, the company has revealed.

Our heroes are, of course, the birds, with each different bird a different character class; the red bird, for example, is the knight, and the yellow bird is the wizard. You'll lead them into battle across a fantasy-themed Piggy Island, defeating the pigs, apparently, on their home turf presumably the story will reveal the whys and wherefores.

It also seems that crafting will feature quite heavily. You'll be able to build your own weapons; according to Angry Birds Nest, these can be items such as a wooden sword, frying pan or "stick thingy with a sponge on top". All characters, gear and potions will be upgradeable, too.

The game is due to soft-launch either today or tomorrow in Australia and Canada, arriving shortly after for the rest of the world, and for Android later this year. This soift launch has roughly similar timing to the Australia/Canada soft launch of Rovio's "Angry Birds for girls", Angry Birds Stella, about which few details are known other than its ridiculous gender specificity.

Valve Shows Off Latest Steam Controller Ahead of GDC

After showing off a rough design update to its Steam Controller at its annual Steam Dev Days conference back in January, Valve has decided, definitively it would appear, to strip the touch screen from the handheld and replace it with a logo-emblazoned home button alongside start and select buttons. And new to the latest prototype design is a protruding d-pad and X, Y, A, and B button layout similar to that of an Xbox controller.

The company showcased the changes on its blog Friday ahead of the Game Developers Conference in San Francisco next week, where Valve will be showing off 10 hand-built iterations of the updated prototype for play testing.

Valve will be prepping 10 hand-built versions of its Steam Controller to bring to the annual Game Developers Conference in San Francisco next week. (Credit: Valve)

The original Steam Controller concept contained a square touch screen with buttons surrounding the edges, while the prototype shown off last year relied on a four-pad touch interface in lieu of installing full-blown LCD screens. But Valve apparently took to heart user feedback and made some tough choices in simplifying the device to make it more in line with modern console controller design.

While looking considerably more polished than past prototypes, the Steam Controller is no longer such a far cry from fellow console game pads without its touch screen and with the addition of a d-pad and traditional button scheme. The insistence on a trackpad-like interface instead of thumbsticks however would still be the most radical aspect of it, and those don’t look like they’re going away anytime soon.

That said, Valve does not sound like it’s finalized its design, and will be using GDC as an opportunity to continue cooking up some more tweaks.

PS4 Sales Tops Xbox One in February, But Not By Much

Sony’s PS4 was the best-selling game console in the U.S. last month, but Microsoft’s Xbox One earned more money.
71shares

In the war of the next-gen video game systems, Microsoft’s Xbox One is still trailing Sony’s PlayStation 4, but the gap is narrowing, according to new data from The NPD Group.

The research firm on Friday reported that the PS4 $399.99 at Amazon was the best-selling game console in the U.S. last month, narrowly beating out the Xbox One $499.00 at Amazon. Microsoft’s new console sold "over 90 percent of what the PS4 sold in terms of unit sales," but thanks to its higher price point, Redmond actually made more money, beating out Sony’s system on a dollar basis, NPD analyst Liam Callahan said in a statement.

In January, PS4 sales were nearly double that of Xbox One.

In a blog post, Microsoft said it sold 258,000 Xbox One units in February, surpassing its 114,000 Xbox 360 unit sales by more than 61 percent. The new sales figures follow this week’s highly anticipated launch of Titanfall.

"Since it launched on Tuesday, the Xbox community has been out in force playing ’Titanfall’ on Xbox Live," Microsoft said. Xbox 360 gamers will have the chance to play Titanfall when it launches on the seventh-generation console March 25.

Meanwhile, total U.S. video game hardware sales saw a 42 percent lift last month, reaching $347 million, due to a more than 60 percent increase in console purchases, NPD said. "Within console hardware, we continue to see strong year-over-year increases due to the success of the Xbox One and PS4," Callahan said.

Overall sales of new hardware, software, and accessories totaled $887 million in February, up 9 percent from the same time last year. NPD estimated that used and rental sales totaled $131 million while digital format sales brought in $512 million, bringing total U.S. video game sales to around $1.47 billion in February.

On the software side, Call of Duty: Ghosts was the top-selling game last month, followed by The LEGO Movie Videogame, NBA 2K14, Thief, and Grand Theft Auto V. Rounding out the top 10 were: Battlefield 4, Assassin’s Creed IV: Black Flag, Lightning Returns: Final Fantasy XIII, Minecraft, and Bravely Default.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

The Insanity of Making Six Retro Games in Six Months
...Or trying to, anyway

Rusty Moyher spent so much of last year building retro games he "blew out" his hands. As part of the Retro Game Crunch challenge, Moyher joined up with fellow developers Shaun Inman and Matt Grimm to develop six 8-bit-style games over the course of six months, based on ideas from Kickstarter backers. It was an ambitious project with tight restrictions and a tough schedule, which led to some overexertion. "We didn’t really limit the amount of hours we were putting into it," says Moyher, who developed repetitive strain injury issues while working on the half-dozen new games. After a few delays, the trio managed to complete the games at the end of last year, and this week the collection is available as a bundle to anyone who missed out on the crowdfunding campaign.

This is what crowd participation looks like for video game development.

On paper, the self-imposed challenge was simple: each month backers would submit a theme, and then vote on which one would actually be turned into a game. The developers would then spend three days building a prototype based on that idea. Backers would check out the prototype, offer some feedback, and the team would spend the rest of the month fleshing out the idea into a fully fledged game. The plan was to do this each month for six straight months. "We were a bit bold," admits Moyher.

The resulting games are as diverse as you’d expect from a collection culled from crowdsourced ideas. When the trio was given the theme "music influences the level," they built a rhythm action game called Wub-Wub Wescue, where you play as a pug rescuing an explorer. It’s a platform game, except the obstacles move according to the music and you can

collect records to slow down the tempo and make things a bit easier. The very first theme challenge was "immortal, learn to die." The result was a puzzle game in which a robot has to find ways to kill himself while avoiding the repair bots that want to fix him back up. It’s deceptively challenging and very fun.

The games also vary quite a bit when it comes to scale and quality. Paradox Lost is perhaps the most impressive game, a sprawling side-scrolling adventure in the vein of classics like Metroid or Castlevania. The theme was "can’t stop time traveling," and the game gives you a gun that lets you travel between three different time periods by shooting special crystals. It really feels like a long-lost NES game, and it’s surprisingly expansive for an experience built in a month.

One of the struggles the team had was getting everything they wanted into each game before their self-imposed deadlines. For a game like Paradox Lost, which is brimming with inventive ideas, leaving it behind to immediately switch to something new was difficult. "I could always spend more time on something," says Moyher, "but whether I should is another question."

A desire to make things as good as possible wasn’t what caused the delays, however. The team didn’t run into many technical issues along the way in fact, from a coding perspective, things got a bit easier as time passed and the Kickstarter backers provided lots of good themes that resulted in clear game ideas. Instead, the delays were caused by unforeseen circumstances: in addition to Moyher’s RSI issues, which forced him to see a physiotherapist, one of the team members also had to leave to help take care of a sick relative. The six games were initially going to be completed by last June, but these issues delayed the final release until the end of the year.

For backers, Retro Game Crunch provided a unique experience, letting them not only have an intimate view into how these games get made, but also a say in what the games would look like. For those who pick up the newly launched bundle, that experience is missing they get a collection of six retro-style games, but without all of the added context of the crowdfunding campaign. What was a yearlong journey for backers becomes something else for new buyers. "It’s a totally different product," says Moyher.

Now that the games are available to a wider audience, Moyher is looking forward to finally getting a chance to work on something else, after dedicating the last year to retro gaming. Currently there are no plans to do anything else with any of the game concepts, such as flesh them out into larger experiences or port them to new platforms (each game is available for Mac and Windows). And though they’re proud of the work that came out of it, it’s also unlikely the team will be doing a similar project anytime soon. "It was just super intense and super hard, and that was mainly due to the schedule," says Moyher. "The rules that we set out for ourselves were less flexible than they should’ve been.

"I don’t think there will be a season two."

Digging for Atari’s ’Corporate Shame,’ The Buried E.T. Games

E.T. wants to go home. But first there will have to be a massive excavation of a city’s garbage dump.

As is part of video-game industry lore, in 1983 Atari ran screaming from its ill-advised E.T. game and hastily and quietly buried millions of cartridges. Somewhere. No one was quite sure where.

It turns out the where was Alamgordo, N.M., and almost certainly deep in the giant city garbage dump. Last year, a team of filmmakers announced they’re working on a documentary about the infamous E.T. game disaster - which cost Atari $500 million and drove it into financial ruin. And at South by Southwest this week, they talked at length about the project and their plans to excavate the games and make their movie.

The filmmakers behind the movie about the excavation of the infamous E.T. game cartridges make a point about why they were buried.

The history of Atari’s disaster is pretty well known. In 1983, on the heels of the unbelievable success of Steven Spielberg’s "E.T.," the suits at Atari ordered a game version. Pronto. They wanted it to hit shelves in six weeks. In an industry where quality mainstream games usually took months, this was a tall order. The result? An effort generally thought to be one of the worst games in history - shallow, ugly, boring. It sold 1.5 million units immediately because of the movie’s success, but then sales ground to a full-stop halt.

Flash forward 30 years and the folks at Lightbox and Fuel Entertainment got together to make a movie about this legend. They got Microsoft on board to distribute it as part of its Xbox film series, and they were off for New Mexico.

At SXSW, Johnathan Chinn, co-president and producer at Lightbox, and Mike Burns, CEO of Fuel Entertainment, explained where they’re at with things. For one, they’re almost certain the games are buried in the city dump in Alamogordo. But even if that turns out to be true, it’s a massive facility, and it will not be a simple matter of digging one hole and declaring victory. The dig could take time, they said, and they’ll want help. They hope that people will show up to assist and, perhaps, cheer them on.

Most likely, they’ll start the excavation - with the permission of the dump, of course - sometime this spring. Perhaps as early as April. Assuming they find the cartridges in short order, the dig could be over quickly. But it could also drag on. Regardless, the movie itself is about much more than just the creation of the video game and its subsequent tarnished history. Instead, the filmmakers said, they realized there was an opportunity to wrap that story around a larger tale of Atari’s rise and fall. From being a company founded by the larger-than-life Nolan Bushnell, which hired the young Steve Jobs and Steve Wozniak, to one whose name and intellectual property has been sold and bought and dispensed with and rescued time and time again.

At the heart of that roller-coaster ride, though, is the misguided attempt to cash in on Spielberg’s theatrical triumph. "My sense is that this is a story of corporate shame," Chinn said. "They just wanted it to go away, but here we are making a film about it. The moral of the story is: Don’t just bury your mistakes."

While there will be a lot about Atari in the film, the real drawing card will be the hunt for the buried games. A good bit of that could be the

film production team’s many trips to and time spent in and around Alamogordo. "I did speak to a bunch of witnesses in Alamogordo, who were kids in 1983," Chinn recalled, "who claimed that they snuck into the landfill and stole cartridges that were totally playable. Other people, including people at Atari, claimed that there wasn’t anything interesting there."

100,000 Minutes of Kaboom!

(Courtesy of AtariAge)

Frequent visitors to AtariAge may know about our weekly gameplay tracker, started by AtariAge member cvga in 2008 and continued by thegoldenband since 2010. Participants in the tracker simply log the amount of time they spend playing games on pre-modern platforms (i.e. anything up to the Dreamcast), and the numbers are then totaled each week to see which games and consoles have gotten the most time.

One of our members, Atarian7, has been on a quest to reach the maximum possible score of 999,999 points in the game Kaboom!. He’s come very close in the past, logging a score of 928,982 in April 2012, and his prowess has even earned praise from Larry Kaplan, the game’s designer.

As of this week, he reached a tremendous milestone, and has now logged over 100,000 minutes of Kaboom since the tracker was founded. That’s more than two months of continuous play! Will Atarian7 reach 999,999 points before he reaches 999,999 minutes?

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Target Admits That It Missed Warning Signs Before Data Breach

Target has admitted that it missed warnings that it was about to be the victim of one of the largest breaches of security in U.S. history. The retail chain came clean after a damning Bloomberg News report claimed that a computer security firm s trap had picked up a hacker trying to access customer information.

The Bloomberg report claimed that Target had installed a $1.6 million malware detection tool created by FireEye and that it also had a team in Bangalore keeping a round-the-clock eye on data to make sure there was nothing suspicious. One of the traps set by the FireEye program was stung by a hacker on Nov. 30 and the Bangalore team did tell the company. However, nothing was done.

Now, a day after the Bloomberg report went live, Target has had to acknowledge that it made a mistake. With the benefit of hindsight, we

are investigating whether, if different judgments had been made the outcome may have been different, a spokeswoman said in a statement, notes PCMag.

Target did admit on Dec. 19 that it was a victim of a security breach, which affected 40 million credit cards and over 70 million customers. Just last month, its fourth quarterly earnings report showed that profits dropped 46 percent over the same time period in 2012. The blow was even harder to take, as it happened during the busy holiday shopping season.

FireEye also issued a statement in response to Bloomberg s claims, saying that it could not publicly confirm who its customers are.

In Target s statement today, the company admitted that it did receive notice of criminal activity.

 That activity was evaluated and acted upon. Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow up, Target stated. Our investigation is ongoing and we are committed to making further investments in our people, processes and technology with the goal of reinforcing security for our guests.

NSA "Hijacked" Criminal Botnets To Install Spyware

While U.S. law enforcement agencies have long tried to stamp out networks of compromised computers used by cyber criminals, the National Security Agency has been hijacking the so-called botnets as a resource for spying.

The NSA has "co-opted" more than 140,000 computers since August 2007 for the purpose of injecting them with spying software, according to a slide leaked by former NSA contractor Edward Snowden and published by The Intercept news website on Wednesday.

Botnets are typically used by criminals to steal financial information from infected machines, to relay spam messages, and to conduct "denial-of-service" attacks against websites by having all the computers try to connect simultaneously, thereby overwhelming them.

In November, Federal Bureau of Investigation Director James Comey told the Senate that botnets had "emerged as a global cyber security threat" and that the agency had developed a "comprehensive public-private approach to eliminate the most significant botnet activity and increase the practical consequences for those who use botnets for intellectual property theft or other criminal activities."

According to the NSA slide published by The Intercept, one technique the intelligence agency used was called QUANTUMBOT, which "finds computers belonging to botnets, and hijacks the command and control channel." The program was described as "highly successful."

Reuters reported in May that U.S. agencies had tapped botnets to harvest data from the machines’ owners or to maintain the ability to issue the infected computers new commands.

The slide leaked by Snowden is the first confirmation of the practice, and underscores the complications for the NSA of balancing its major

mission of providing eavesdropping capability with the less well-funded missions of protecting critical national assets and assisting law enforcement.

The Top Secret slide was marked for distribution to the "Five Eyes" intelligence alliance, which includes the United States and Britain.

The NSA declined to confirm or deny the existence of the program. It is not known if the botnets hijacked by the agency were in other counties or in the United States, or if the botnets could have been recaptured by criminals.

Many botnet operations disable the machines' security software, leaving them vulnerable to new attacks by others.

In a written statement, an NSA spokeswoman said: "As the President affirmed on 17 January, signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes.

"Moreover, Presidential Policy Directive 28 affirms that all persons - regardless of nationality - have legitimate privacy interests in the handling of their personal information, and that privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities."

The Intercept article and supporting slides showed that the NSA had sought the means to automate the deployment of its tools for capturing email, browsing history and other information in order to reach as many as millions of machines.

It did not say whether such widespread efforts, which included impersonating web pages belonging to Facebook Inc and other companies, were limited to computers overseas.

If it did pursue U.S. computers, the NSA also could have minimized information about those users.

The NSA Posed as Facebook To Better Spy on You

You re probably already well aware that the National Security Agency is spying on you. A new report from The Intercept reveals yet another place they re doing it.

The NSA pretended to be Facebook you know, that 500-million person social network so it could trick you into downloading invasive malware. Per the piece:

"In some cases the NSA has masqueraded as a fake Facebook server, using the social media site as a launching pad to infect a target s computer and exfiltrate files from a hard drive," Ryan Gallagher and Glenn Greenwald report. "In others, it has sent out spam emails laced with the malware, which can be tailored to covertly record audio from a computer s microphone and take snapshots with its webcam."

It s a variation on a common scheme called phishing, in which an entity

poses as an official site, gains your trust and then exploits it. Usually, the perpetrators are small-time crooks, and not the U.S. government.

These particular tactics were apparently once only reserved for a small number of difficult targets who couldn t be monitored via traditional wiretaps. But according to documents obtained by The Intercept, the NSA has recently expanded this technology so that these little malware mines around the internet, dubbed implants, can scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually.

In other words, the NSA designed a surveillance system that skirted actual human oversight so that they could spread malware to millions of computers. Malware that allows them to see everything you ve saved on your computer. Not cool.

Even worse? This type of spying actually weakens computer security systems, immediately making any NSA target vulnerable to third-party attacks, a malware expert told The Intercept.

The NSA declined to answer specific questions about this project. As the president made clear on 17 January, the agency said in a statement, signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes.

These revelations come just on the heels of the South by Southwest Interactive conference, which hosted a talk with Edward Snowden on Monday. The former NSA contractor and whistleblower urged technologists to begin designing products which focus on individual security.

Technologists, hurry up, please.

162,000 WordPress Sites Used in DDoS Attack

More than 162,000 popular and clean WordPress sites were recently used in a large-scale distributed denial of service attack (DDoS) that exploited the content management system s pingback feature.

While the WordPress team is aware of the issue it s not expected to be patched as it s a default feature on WordPress, not a flaw, meaning it s a problem that will likely be left up to site developers to mitigate.

Attackers abused a number of sites that have the feature, essentially XML-RPC requests that make it easy for blogs to cross-reference other blog posts, enabled.

Daniel Cid, the CTO of security firm Sucuri, described the attack, which took down a undisclosed website belonging to one of the firm s clients, in a blog post on Monday.

According to Cid the attack appears to have used the application-layer (Layer 7) HTTP Flood Attack style of DDoS, which are harder to detect as the requests look like they re coming from legitimate sites.

In this case they were legitimate sites, 162,000 of them, sending random

requests at a very large scale to the site s server, each one with a randomized value that bogged their site down by bypassing their cache and mandating a full page reload each time.

Unlike conventional DDoS attacks that use NTP and DNS, this attack, reflective in nature, used the websites as indirect source amplification vectors. While WordPress sites were the victim this time around, experts say any site could technically be tweaked to dole out this kind of flood attack.

We would likely have detected a lot more sites, but we decided we had seen enough and blocked the requests at the edge firewall, mostly to avoid filling the logs with junk, Cid wrote.

Since the POST requests were sent to /xmlrpc.php request they re easy to find in logs, so Cid is encouraging WordPress developers to check theirs to ensure that their sites aren t vulnerable and attacking other WordPress sites.

Developers can also use a scanner the firm came up with this week to check its logs to tell if certain WordPress sites are DDoSing other websites.

If found, Cid claims users can remedy the situation by either disabling XML-RPC pingback or creating a plugin to add a filter to block these kind of pingbacks. Users interested in learning more on how to do that can head over to their blog.

As Johannes B. Ullrich, chief technology officer at the SANS Technology Institute adds, removing xmlrpc.php is not a recommended option as it will break a number of other features that will use the API.

Bitcoin Exchange Mt. Gox Files for U.S. Bankruptcy as Death Spiral Continues

The Mt. Gox death spiral continues. The big-name bitcoin exchange has now filed for bankruptcy protection here in the U.S., as well as Japan, and hackers are saying they ve uncovered evidence of fraud at the Tokyo-based company, after allegedly breaking into a website controlled by its CEO.

Mt. Gox was once the most popular site for buying and selling the digital cryptocurrency bitcoin. But last month, after months of complains from users unable to withdraw funds, the company took its entire operation offline and filed for bankruptcy protection in Japan. The new U.S. filing, made in Texas, is meant to protect the company s U.S.-based assets, as reported by The Wall Street Journal. Mt. Gox is facing a class-action lawsuit filed in Illinois, and it has long been involved in a $75 million lawsuit with another bitcoin company, called CoinLab.

The ongoing travails of Mt. Gox act as a metaphor for the bitcoin world as a whole. Though the digital currency is beginning to remake the way the world moves and stores money, many of the companies and individuals that first pushed the technology into the mainstream are now struggling to come to terms with government regulations and the realities of doing business.

At a press conference last month, Mt. Gox CEO Mark Karpeles admitted that the company lost around 750,000 of its customers bitcoins worth around half a billion dollars. He blamed a known issue in the bitcoin protocol that enabled hackers to trick the company s software into thinking

transactions failed. Apparently, Gox s accounting software didn t deal with this flaw and could be tricked to send repeated bitcoin payouts to the same customers.

How Mt. Gox could have lost so many bitcoins without noticing remains a matter of speculation, and many suspect foul play on the company s part, not just mere incompetence. Among them are the hackers that hijacked Karpeles personal website and published a file they claim contains data acquired from the company s servers. Included in the file was an Excel spreadsheet showing a balance of 951,116 bitcoins.

The hackers, who also hijacked Karpeles Reddit account, claim the document proves that Mt. Gox is still in control of those bitcoins. But given Mt. Gox s claim that the bitcoins were stolen without anyone at the company noticing, it would make sense that the company s official balance sheets still show a much larger number of bitcoins. Ultimately, even if the document is authentic, it proves nothing one way or the other.

Many Reddit users claim to have found their own transaction data in the spreadsheet, suggesting that the materials are authentic. But Forbes reporter Andy Greenberg warns that the zip file may contain malware designed to steal bitcoins and cautions people not to download the file. Neither Karpeles nor Mt. Gox responded to a request for comment about the spreadsheet s origins or authenticity.

The alleged hack follows a number of other leaks and hacks from the company, including a leaked internal document about the missing bitcoins and supposed copies of the code used to run the exchange. Meanwhile, Bitcoin users are dealing with the bankruptcy in their own way: by creating a new currency to buy and sell rights to the lost bitcoins, should they ever be recovered.

Mind Your Wallet: Why the Underworld Loves Bitcoin

Criminals may already have made off with up to $500 million worth of Bitcoin since the virtual currency launched in 2009 and you can double that if it turns out they emptied Mt. Gox.

Internet criminals, security experts say, are attracted to Bitcoin because of its stratospheric rise in value, because it s easier to steal than real money, and because it s easier to trade with other criminal elements. But, they add, Bitcoin will survive the damage.

 It s just growing pains, says Keith Jarvis, a security researcher at Dell SecureWorks. Bitcoin is large enough and has enough momentum behind it to survive any public relations damage from this (Mt. Gox) case or anything else.

The fall of Mt. Gox, the Tokyo-based exchange that filed for bankruptcy last month after saying it lost some 850,000 bitcoins to hackers, is certainly the virtual currency s biggest crisis.

But data collated by Reuters from specialist Bitcoin industry websites and Internet forums shows that more than 730,000 bitcoins were already missing to theft, hacking, cyber-ransom payments and other apparently criminal pursuits before Mt. Gox s collapse. That s nearly 6 percent of all bitcoins and doesn t include dozens, possibly hundreds, of

unreported cases of individuals who have lost bitcoins from their computers or online exchanges to hackers.

For sure, there s no way of telling who has these missing bitcoins or whether they were converted to real money when the price was much lower. And of course some bitcoins may have been counted twice if criminals stole them from each other or if they were put back into circulation and stolen again.

But there s no question that bitcoins have attracted the attention of cyber-criminals as a currency and an asset worth stealing.

A study by Pat Litke and Joe Stewart of Dell SecureWorks showed that as the price of bitcoin soared beyond $1,000 last year, so did the number of viruses designed to steal bitcoins from wallets programs that hold bitcoins on people s computers or smartphones. Of the 140 types of such software, more than 100 appeared in the past year.

Writing such viruses, Stewart says, is easy. There s no sophistication involved in the storage of bitcoin in wallets. As for malware, it s some of the easiest stuff to write.

Indeed, this cyber pocket-picking wasn t criminals first foray into bitcoins. Initially, they focused on using their control of large networks of infected computers called botnets to make their own bitcoins.

Bitcoins are created through a mining process where a computer s resources are used to perform millions of calculations. For a while, says Kirill Levchenko, a researcher at the University of California, San Diego, criminals added malware to their botnets to turn infected computers into bitcoin miners.

This triggered predictions of doom for bitcoin that the criminals would take over the mining of bitcoin through botnets and bring the whole currency crashing down. But as bitcoins become harder to mine according to an algorithm that slows down their production the more people try to create them this approach has proved less profitable.

In 2012 and 2013, says Danny Huang, another researcher at the University of California, San Diego, botnets earned at least 4,500 bitcoins, a relatively small sum compared with the total produced. Few botnets are mining bitcoins now, he says.

Instead, criminals have turned to stealing them from wallets or, more lucratively, from exchanges.

According to data compiled last year by academics Tyler Moore and Nicolas Christin, of 40 exchanges tracked, 18 had closed, with customer balances wiped out in many cases not always, they point out, due to fraud. Since then, according to public reports, more than a dozen others have been hacked.

Cyber-criminals have also made use of the ease with which bitcoins can be traded without any third party such as a bank or an online payments service like PayPal to use it as at least one way of paying for services among themselves.

 Bitcoin made it much easier for them, because they have to trust each other even less. Even complete strangers can cooperate, said Juraj

BednÆr, a Bitcoin security expert in Slovakia.

But while Bitcoin has its advantages, it s not a perfect tool for the bad guys.

Take, for example, ransomware. Viruses that encrypt data and then demand payment for a key to unlock it have become increasingly sophisticated, says Dell SecureWorks Jarvis.

The most successful: CryptoLocker, which Jarvis believes is run by a Russian-speaking gang who are also behind a botnet called Gameover Zeus that targets financial websites.

Bitcoin often appears on CryptoLocker as an option for victims to pay up. Its appeal, BednÆr says, lies in the fact that it needs no third party for the transaction to work.

But there have been problems. For one thing, the type of person to be infected by a virus wasn t likely to be the type who is technologically savvy enough to be familiar with Bitcoin. Also, as Bitcoin rose in value, it became a more expensive option for the victim, forcing the criminals to lower their ransom demands to match prevailing exchange rates.

Then there s Bitcoin s transparency. All transactions are visible, and while they re just digits and letters, in theory they could be connected to an individual and the entire history of all the bitcoins transactions traced.

Italian computer engineer Michele Spagnuolo, for example, was able to trace a number of ransom payments for CryptoLocker. The gains have been impressive: He and academics from Politecnico di Milano speculate that up to 6,757 bitcoins then worth around $6 million could be linked to those behind CryptoLocker late last year. That estimate of their total takings, he says, could be very conservative.

But the fact that such payments can be traced would raise a red flag for cyber-criminals, says Daniel Cohen of RSA, the security division of EMC, even though there are online services that can launder bitcoins to hide their origin. Sure, there are Bitcoin laundering services, but still if I tie a wallet to an identity I can see every single movement, he said.

And, ironically, the success that some criminals have had in stealing bitcoins has made them less appealing to the underworld. RSA s Cohen says his team monitoring underground forums has noticed that criminals lately see Bitcoin as volatile, seizable and, with the recent thefts, unsafe.

That s not to say Bitcoin is out of the woods.

While the protocols underlying Bitcoin have proved themselves to work, the weak links have been the software containing the wallets, whether on exchanges or on individuals computers.

 The attacks on the exchanges did not in themselves indicate any particular weakness of Bitcoin per se, but rather exploiting vulnerabilities within the exchanges, says Raj Samani of Intel s Internet security company McAfee.

Such holes are being addressed, says Dell SecureWorks Stewart, pointing to such innovations as hardware wallets to replace software ones. We re just going to have to get into that mode of thinking, he says.

For now, Bitcoin remains a vulnerable target.

That was illustrated when hackers breached Mt. Gox s servers and its owner s blog this week to post files purporting to be Mt. Gox s transactions in Bitcoin stretching back to 2011.

Amid the files lurked another surprise awaiting the unwary: a Bitcoin-stealing virus.

Facebook’s Menlo Park Headquarters Evacuated After Threat

The headquarters of social media giant Facebook was temporarily flooded with officers and cordoned off Tuesday evening after a threat against the company was called in to authorities, Menlo Park police said, but the threat was quickly cleared.

The threat was originally called into the San Francisco Police Department around 7 p.m., said Menlo Park police Cmdr. Dave Bertini.

The department transferred the call to Menlo Park officers, who went to the campus and closed off the entrance with tape. Officers searched the campus, while the company asked its employees to stay put before police could prove or disprove the threat.

"At this point, we’re not even sure the call was meant to be for the Menlo Park campus," Bertini said.

Officers did not find anything at the campus, and Facebook eventually shuttled its employees home.

Bertini added that he could not say what the threat was, only that it was proven to be "non-credible."

The company, founded in 2004, has more than 6,000 employees. Thousands of those workers report to the company’s main campus at 1601 Willow Avenue, an address that was rechristened as "1 Hacker Way" after the company took over the old Sun Microsystems campus.

Last week, Menlo Park’s city council voted last week to allow the company to pay about $200,000 a year to the city to fund a full-time police officer who would be stationed near the new campus.

Twitter Suffers Service Issues

Twitter reported a service outage Tuesday, saying most people were having issues accessing its widely used messaging service on the web and through mobile applications.

 We re looking into it. We ll post updates to our status blog as we have them, company spokeswoman Christina Thiry told Reuters via email.

Further details on the cause of the outage were not immediately available.

U.S. Said To Relinquish Control of Internet Address System

The U.S. plans to hand over control of the system for assigning website addresses to a non-government entity, an Obama administration official said.

The agency has asked the non-profit Internet Corporation for Assigned Names and Numbers to convene interested groups from around the world to develop a proposal to transition the system, said Lawrence Strickling, administrator of the National Telecommunications and Information Administration in a phone call with reporters today.

We will not accept a proposal that replaces the NTIA role with a government or intergovernmental organization, Strickling said.

The move represents the final phase in the U.S. government s effort to privatize the backbone of the Internet that provides websites with their unique identifiers, which are essential for users to find what they re looking for online. U.S. control over Internet functions has come under attack from privacy advocates and foreign governments in the wake of revelations about National Security Agency spying.

NTIA plans to allow its contract with the Internet Assigned Numbers Authority to expire on Sept. 30, 2015, Strickland said. It isn t clear yet what organization or groups will take over its responsibilities to maintain unique codes and numbering systems that are used in the technical standards that drive the Internet.

The U.S. is fulfilling a pledge it made as far back as 1998 to relinquish control of the Internet s domain name system, Fadi Chehade, president and chief executive officer of ICANN, told reporters on the conference call.

We thank the U.S. government for its stewardship, for its guidance over the years, Chehade said. And we thank them today for trusting the global community to replace their stewardship with appropriate oversight mechanisms.

How to Avoid Phishing Scams

Phishing is an age-old Internet pothole. It s survived since the early ages of AOL chatrooms for one simple reason: It really works. The setup is simple: A bad guy poses as a trusted entity online to steal your personal information.

Just ask the U.S. government, which we recently learned has adopted phishing techniques to spy on millions of people. It s probably about time you learn a little about how to avoid getting phished yourself, no?

Phishing is the online version of being conned. Imagine Leonardo DiCaprio s character from Catch Me If You Can but less charming. These scammers sit at their computers and pretend to be legitimate trusted companies (like Microsoft or Netflix) as a way of tricking you into handing over personal details like login info, credit card numbers and

sometimes even money.

Phishing comes in many forms: emails that seem like they re from Wells Fargo or Facebook, instant messages or communications from people on popular social networks like Twitter or Facebook. It all starts with a link. Once you click it, you re redirected to a pharming website that looks identical to whichever company the scammer is posing as. You re then prompted to enter your login information.

From there, scammers might lure you to other sites or try to trick you into downloading attachments that unleash viruses, keystroke-tracking software or other malware.

You are most certainly an intelligent human being who can smell the stink of a sleazy salesman or a tourist trap. But when it comes to phishing, you might be less savvy than you think. Last year, researchers at North Carolina State University asked a group of 53 undergraduates to distinguish malicious emails from legitimate ones, and nearly everyone in the group failed. Keep in mind that these were students, meaning that they were likely young Internet natives. In other words, scammers are getting just as sophisticated as the people they re exploiting.

OK, OK. What are a few things I should look out for?
Glad you asked! Here s the super-simple version:

Don t click on hyperlinks in emails from people you don t know. This piece of advice is a little less obvious than you think. Yes, your mother, husband, sister and aunt are not trying to send you spam. But that doesn t mean that their email accounts aren t vulnerable to being hacked. So always make sure to hover your mouse over the linked phrase in question. Usually the address of the item will pop up in a gray box at the bottom-left corner of your browser. Like so:

If it doesn t look familiar, steer clear.

Also, smartphone operating systems are currently much less vulnerable than those of your computer. So if you re unsure about something, try opening it on your mobile device (Apple products are usually less vulnerable to viruses). This might protect you from getting malware, but if you start typing in your bank account number on a phony site, you re still in a world of trouble.

Verify your web URLs. Whenever you visit a site that requires you to enter sensitive information (credit card numbers, your Social Security number or other financial information), check the URL in your search bar. It should show https:// rather than http://, and usually a secure connection is displayed with a little padlock image like the one below. You can double-click the padlock to see the security info that lets your browser verify that the site you re connecting to is what you think it is. SSL stands for Secure Sockets Layer. It keeps all the communication between your browser and your websites servers private and secure.

Just completely ignore pop-up windows. Pop-up windows are inherently sketchy because without a bar that displays a site s URL, you can t actually verify that it s a secure site. So don t enter your sensitive info into one, and always make sure to click the X in the top corner of the box to get rid of them. Clicking the Cancel button can sometimes send you to a link, or automatically install malware.

Look out for weirdly formal language. Modern companies don t usually

write royal English or handpick their customers to receive thousands of dollars. If anyone calls you Sir or Madame in an email and she s not the Dowager Countess from Downton Abbey, it s probably a scam.

Do I have to, like, download some software?
Yeah, that d be a good idea.

First and foremost, you should get antivirus software that will help protect you from bad stuff floating around online. The type you should choose depends entirely on your operating system. Here s a good resource for PC owners. And if you don t want to spend any money, this is a legit list of free services. Whatever you choose, make sure to keep it up to date. Your web browser is much more susceptible to a hijacking if your security software goes stale.

Anti-spam software isn t essential, but it lowers your chances of falling victim to a phishing attack, since many of them come in spam form. PC Mag has an extensive list here. And many browsers provide add-ons that help protect your computer. Chrome, for instance, has a free AdBlock extension. So does Firefox.

And then there s anti-spyware software. Unlike malware, which is intended to damage or disable your computer system, spyware infiltrates your hard drive to collect information. This is something that Windows owners, above all others, must be cautious of. Here s a list of free anti-spyware software that can prevent the problem before it happens.

This is really overwhelming.
I feel you. And this is the simple version.

Why can t companies just make products more secure from the get-go?
You re not alone in asking that! Former NSA contractor and whistleblower Edward Snowden said he thinks they should, too, at South by Southwest this week.

That doesn t make me feel any better.
Sorry!

Asus Chromebox: A Tiny, Cheap, Very Useful Computer

I roll my eyes when people claim that we re living in the post-PC era.

I mean, we do live in the post-VCR era. And the post-zeppelin era. And the post steam locomotive era.

And it s true that sales of Windows PCs are dropping a few percent a year, thanks to the rise of smartphones and tablets. But to say that nobody has them anymore? Yeah, no.

That s not to say that things aren t changing. Our lives are moving online. Recently, a friend said Whoa, you almost forgot your laptop! You d lose all your data your whole life! But actually, I wouldn t lose much of anything. Almost every important thing on my laptop is stored online and backed up automatically: email, calendar, address book, documents, photos, and so on.

That s all the setup you need to understand the appeal of the new Asus

Chromebox. It s among the least-expensive desktop computers ever sold $180 and certainly among the smallest. It s a 1.7-inch-tall square slab, 4.9 inches on a side; the computer isn t much bigger than its own power brick. You could slip this thing into a coat pocket on your way out the door. It could pass for a generously sized brownie.

That price and those dimensions, of course, account only for the computer itself. Mouse, keyboard and monitor aren t included. Those accessories might cost another $75 or more. Or less, depending on what you ve got lying around your house and how cheap a shopper you are.

The big thing, though, is that the Chromebox doesn t run Windows or Mac OS X. The Chromebox is the desktop version of Google s Chromebook laptop concept, which means that it s intended exclusively for doing things online.

Yes, it s true: A Chrome PC can t run traditional programs like Photoshop, Microsoft Office, iTunes, Quicken, or Minecraft. (Some would say, Thank goodness.)

It runs the Flash plug-in, but it can t run browser plug-ins like Java or Silverlight, which means that a few web-based games and video playback sites won t work. If you hook up a webcam, you can conduct video chats using Google s Hangouts feature but you can t use Skype.

What you can do is check email, build spreadsheets, watch movies on Netflix, chat up friends on Facebook, share photos on Instagram, stream music on Pandora, surf the web and so on. (That quotation comes from fellow Yahoo Tech columnist Dan Tynan s terrific introduction to Chromebooks here.)

And, of course, you can use all of Google s online products: Google Docs (for working with Microsoft Word and Excel documents), Gmail, Google Maps, Google Calendar, Google+ and so on.

There are apps that run on Chromebooks and Chromeboxes, but not very many, and they re not as complete, polished or famous as their Windows and Mac forbears. For most people, they re a fairly unimportant part of the Should I buy a Chrome machine? calculation.

Why buy Chrome?

Chrome computers are cheap, fast, easy to use and secure (no viruses!). Chrome machines make phenomenal kitchen computers, for example great for quick lookups, debate-settling, waiting-for-the-cable-guy surfing. They re fantastic for kids, whose lives (including schoolwork) are primarily online these days. And for anyone or any family, a Chrome machine makes a superb second or third computer.

The new machine, the Asus Chromebox, is everything it s supposed to be. It s incredibly inexpensive. It s fast to set up and fast to respond. It has no fan, so it s completely silent. It has plenty of connectors: four USB jacks (the fast 3.0 kind), an HDMI jack for connecting a TV, a DisplayPort for a projector or a monitor, an Ethernet jack, audio, and even a slot for the memory card from your camera. WiFi is, of course, built in.

There s 16 gigabytes of storage inside (many apps can store themselves on the box, for use when you don t have an Internet connection) but there s also 100 gigabytes of storage waiting for you online from Google.

You get that massive storage locker at no charge for two years. That s a lot of Word and Excel documents. (You can work with those, remember, thanks to the free Google Docs site online.)

A faster version of the Asus is coming in April for $370 doesn t really seem worth it and a matching keyboard/mouse package is coming soon for $50.

The Chrome computer idea appeals to an awful lot of people, and it s picking up speed. But most of those people buy Chromebook laptops. Why would anyone buy a desktop version of the same thing, one that you can t pick up and use on the plane?

There are reasons.

First, there s a slight price advantage. The Asus Chromebox costs $180; Chrome laptops cost $200 or $250 and up. (Samsung and others make Chromebox desktop computers, too. But they re bigger than the Asus and more expensive $300 and up.)

Second, a desktop version lets you plug in any monitor you want. Any brand, any size. Two simultaneously, actually. You can even plug in a TV, courtesy of the Chromebox s HDMI jack. (Then again, the laptop versions let you plug in an external monitor of your choice, too.)

Third, the Asus is so tiny you can mount it on the wall heck, you can duct-tape it to the back of your monitor. That opens up new possibilities if you have cramped or cluttered working quarters, or if you plan to connect it to your TV for Netflix and movie watching.

Those are pretty flimsy reasons, actually. If you re in the target demographic for a Chrome machine for example, if you oversee children, a school, a library or a home with more than one room you re probably better off with a Chrome laptop a Chromebook like the $200 Acer Chromebook shown here.

But choice makes the world go round. The Chrome PC idea is, in its way, a beautiful addition to the technology world, because things that are fast, cheap, simple, reliable and good at what they do are always welcome. And while more people buy laptops than desktops these days, it s nice to know that a desktop option is there.

Incidentally: I ve heard, on occasion, the following logic used to dismiss the whole idea of Chrome computers. OK, it s cheap but it s not a real computer! It s like buying a new car for $1,000 that can t make left turns.

Is that the right analogy, though? Is a computer that can t run Windows or Mac programs as crippled as all that?

No. In a world where a new car costs an average of $20,000, a Chromebox (or Chromebook) is more like getting a Smart car two-seater for $1,000. You won t be hauling lumber from Home Depot in it, but it s a terrific deal and most days, it ll get you where you want to go.

Have you ever been on the phone with tech support, and the IT dude or dudette asked you what web browser you were running, and you panicked and realized that you had no idea, and also you weren t sure where that information could possibly be, so you start shuffling papers around on your desk, stammering into the receiver, trying to buy time, and then you just hang up the phone?

Well, panic no more, friend: A single-serving website called WhatsMyBrowser is here to help. Visit WhatsMyBrowser.org and voilà! all your pertinent browser information pops up. In addition to identifying your browser, the website also gives you your computer s operating system, tells you whether you have cookies enabled, and displays several other pertinent bits of information that the IT department might need.

The site also generates a unique web page that you can copy and send to whomever you re working with. Pretty, right?

In rigorous tests here at the Yahoo offices, WhatsMyBrowser was able to correctly identify the versions of Chrome, Firefox, and Safari on my laptop. No need to dig through menus on your PC: Just visit the website and you re set.

Now, this is not the first website to perform this task for you. Competitors like Support Details let you quickly email your results directly from the site, and WhatIsMyBrowser.com gives you more information, including an IP address. Those are more robust options that prioritize density over design.

WhatsMyBrowser.org, however, is cleaner and easier to navigate than any other site like this that I ve seen. It also puts the sharing information right up top. My advice: You should bookmark this page or at least one like it! for the next time you ve got to wrestle with tech support. Because the question What browser are you using? shouldn t send a cold shiver down your spine.

Microsoft Is Paying Windows XP Users To Jump Ship

The end of support for Windows XP is drawing ever closer, and Microsoft is sparing no expense making sure users move out of the outdated platform.

In the company’s latest move, it’s now offering Windows XP users $50 (about £30, AU$55) in credit towards any Windows 8 tablet, laptop or all-in-one desktop at the Microsoft Store.

Alongside the gift card, Microsoft is also giving away 90 days of premium support for no extra charge to help customers make the transition. The service includes 24/7 phone and chat support to help with getting set up on a new PC.

Finally, the Redmond firm is extending a free data transfer service through Laplink. The data migration service will help users move over everything on their hard drives to a new machine, including photos, videos, music, and other files for free.

The offer is only valid from now to April 30, so act quickly.

Microsoft has slowly been bringing down the curtain on Windows XP. Along

with a final patch coming April 8, Security Essentials on the old operating system will no longer be supported.

After losing the built-in firewall and security suite, the company has promised to continue providing anti-malware support through July 2015.

Third-party vendors have promised to continue protecting Windows XP with their own anti-malware solutions. However, without any more official security patches coming from Microsoft, it’s clear the sun is setting on the old OS.

Inventor of the Web, Tim Berners-Lee: The Web Should Reflect Human Rights

The World Wide Web celebrates its 25th birthday March 12, 2014. And there s nobody better to discuss that milestone than the man who invented the web s protocols, Sir Tim Berners-Lee (yes, he s been knighted).

In this interview, conducted at SXSW this week, Sir Tim and I discuss where the idea of the web came from and what inspiration he took from previous systems and ideas.

As Berners-Lee points out, many people pushed back on the idea at first. While the Internet existed 25 years ago, people were still information and systems hoarders. They didn t, at first, see the advantage of exposing all their data to the world.

But why did Berners-Lee make entering web addresses so clunky? He explains what the http:// in front of every web address means and why it was important in the early days.

The web at 25, Berners-Lee says, is like a young adult. It s independent, a thing unto itself. It has rights, though, and responsibilities. Berners-Lee also thinks the web should reflect accurately the rights (and responsibilities) of all who use it. There are certain rights that should be more enshrined, he says.

He notes that the web can be a tool for both freedom and oppression. Some countries use the web to take power away from citizens, to spy on them, he says. He notes that corporate control of the web, or of laws that affect it, can be very bad for the web. Corporate-sponsored laws that restrict information flow will continue to pop up, he predicts.

Berners-Lee said that, 25 years ago, he had no idea the web would be so important and so influential in the growth of business and society. He d like to see engineers use more of their social intelligence to build websites that will be used to interact with people from other cultures, to combat xenophobia and ignorance.

But what really dismays Berners-Lee is the growth of spam email. It s a waste of bandwidth and time, he says.

Looking to the future, Berners-Lee is excited about the switch from static web pages to sites that can be programmed just like a computer. That s a massive change, he says. It s leading to real-time communication among web pages, and a new way of making powerful things.

In the next 25 years, Berners-Lee would like to see the web give people

control over where their data is stored. And, of course, to making sure that the underlying infrastructure is free and that it supports, not hinders, people s rights.

Tim Berners-Lee: The Web Needs Its Freedom

Today is a landmark anniversary for Tim Berners-Lee. In March 1989 he wrote a proposal to his employers at CERN for a somewhat abstract "global hypertext" system he called Mesh. A year later he re-named that system the World Wide Web. It caught on.

A quarter of a century later, Berners-Lee is like a proud father, seeing his baby all grown up and making its way in the world without him.

"I feel a certain amount of inventor’s pride," he tells CNN. "My greatest pride has been the spirit of collaboration we’ve had for the last 25 years."

He’s watched the Web grow through a carefree childhood and turbulent adolescence, reaching the kind of age when things suddenly get more serious, and it’s time to make some important decisions about the future.

"At 25 it’s more like a young adult," he explains. "Suddenly it needs its independence; young adults are at the stage when they’re looking for freedom, and in terms of what they do they’re asserting their rights. When (systems) break the whistle blower is the person who saves society by pointing out something that nobody else will.

"Now, 25 years on, Web users are realizing they need human rights on the Web ... We need independence of the Web for democracy, we need independence of the Web to be able to support the press, we need independence of the Web in general. It’s becoming very important to sort out all that."

Recent years have been marked by growing pains. Revelations of mass surveillance by the NSA and other agencies have caused international outrage. Arguments over net neutrality persist and copyright wars pitching open-net activists against mainstream creative industries have grown bitter, with Berners-Lee himself criticized at times. The stock and use of illicit material has grown with the dark net.

Berners-Lee is clear that our ability to speak and associate freely is under threat. The widespread data gathering of the NSA revealed a "broken" system, he believes, and he praises whistle blowers like Edward Snowden whose leaks expose the excesses.

"When (systems) break the whistle blower is the person who saves society by pointing out something that nobody else will, because it’s illegal," he says. "One thing I’d like to see built in the future is an international convention and international respect for whistle blowers."

If spying is one threat, Berners Lee believes censorship is another. He recalls the situation in Egypt, where the Internet was cut off at the height of anti-government protests in January 2011. "For a lot of people that was the first time they realized you could turn it off, and they asked themselves, who could turn it off for me?" he says, adding that "turning off the Internet is more or less a signal that the regime does

not trust its citizens and that the regime is on the way out."

At 58, Berners-Lee is not taking a back seat. Having invented the Web once, he hopes to re-invent it through the "Web We Want" initiative, aiming to create a universal "Internet Users Bill of Rights."

Key targets of the manifesto include spreading net access to the nearly two thirds of the world that still doesn't have it. Establishing clear regulations is also a priority, as is the protection of personal user information.

Berners-Lee still enjoys enough power over his creation to make big changes realistic, through two authorities he founded and continues to lead. The World Wide Web Consortium (WC3) determines standards for all Web infrastructure, backed by the world's leading academic institutions and software developers. The Web Foundation manages the spread and ethical application of the Web, bringing pressure to bear on governments through initiatives such as The Web Index, which ranks nations by Internet access standards.

The Web We Want campaign will rely on mass mobilization across industries, nations and activist bodies to succeed, but Berners-Lee is confident of fostering a spirit of cooperation. He has seen it before and considers it the Web's greatest accomplishment.

"It's really a story of collaboration, people working painstakingly on getting protocols right ... There's an international spirit that ignores boundaries," he says.

As for what the Web will look like over the next 25 years, as it enters its middle age, Berners Lee sees a smarter Web emerging, with users empowered by the huge amounts of personal information collected as part of the "Web of data" - information that could help personalize our Web experience.

"People are worrying about what other people are doing with their data," he says, "but they haven't realized what they can do with their own data."

As we grow more connected to, and reliant on, the Web, so the potential for abuse increases. How we use such a powerful tool amounts to a test of our species, says Berners-Lee, but it's one he is confident we can pass together.

"In general the Web enables humanity to be more powerful and that power can be used for good things and to do horrible things - but on balance when it comes to humanity I'm a tremendous optimist."

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of

each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.